UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

WILLIAM SPEARMAN, BRITTNI LINN, JESSICA ALEXANDER, CHRISTOPHER SANGMEISTER, TAYLOR VETTER, NICHOLE ALLOCCA, KAYLI LAZARD, and BRIDGET CAHILL, individually and on behalf of all others similarly situated, Plaintiffs, v. NELNET SERVICING, LLC Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs William Spearman, Brittni Linn, Jessica Alexander, Christopher Sangmeister, Taylor Vetter, Nichole Allocca, Kayli Lazard, and Bridget Cahill ("Plaintiffs"), on behalf of themselves and all others similarly situated, assert the following against Defendant Nelnet Servicing, LLC ("Nelnet" or "Defendant") based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Plaintiffs bring this class action against Nelnet for its (i) failure to properly secure and safeguard highly valuable, protected personally identifiable information, including without limitation, names, addresses, email addresses, phone numbers, and Social Security numbers (collectively "PII"); (ii) failure to comply with industry standards to protect information systems that contain PII; (iii) unlawful disclosure of Plaintiffs' and Class Members' PII; and (iv) failure to provide adequate notice to Plaintiffs and other Class Members that their PII had been disclosed and compromised.

2. Nelnet is one of the largest student loan servicers in the United States, servicing 589 billion in student loans for over 17 million borrowers.

3. In addition to servicing student loans, Nelnet provides online technology services such as web portal and payment processing services to other student loan servicers, including EdFinancial and the Oklahoma Student Loan Authority ("OSLA").

4. On August 26, 2022, Nelnet began publicly notifying state Attorneys General and 2,501,324 impacted current and former Nelnet account holders that the PII of the 2,501,324 impacted individuals had been accessed and stolen by an unauthorized third-party (the "Data Breach").

5. By August 26, 2022, Nelnet had known of the data breach for over a month but had failed to notify a single impacted individual. Nelnet chose to notify individuals via U.S Mail in letters entitled "Notice of Security Incident."

6. As a result of Nelnet's failures and lax security protocols, hackers gained access to Nelnet's computer systems and/or servers and were able to steal the personal information of millions of customers, including their Social Security numbers, phone numbers, emails, and addresses (the "Data Breach").

7. The Data Breach was a direct and proximate result of Nelnet's flawed online system configuration and design and Nelnet's failure to implement and follow basic security procedures.

8. Because of Nelnet's failures, unauthorized individuals were able to access and pilfer Plaintiffs' and Class Members' PII.

9. As a result, Plaintiffs and Class Members are at substantially increased risk of future identity theft, both currently and for the indefinite future. Plaintiffs' and Class Members'

PII, including their Social Security numbers, that were compromised by cyber criminals in the Data Breach, is highly valuable because it is readily useable to commit fraud and identity theft.

10. Plaintiffs, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, breach of confidence, invasion of privacy—intrusion upon seclusion, violations of consumer protection statutes of their home states, violations of data protection statutes of their home states, and injunctive relief claims.

11. Plaintiffs seek damages and injunctive relief requiring Nelnet to adopt reasonably sufficient practices to safeguard the PII that remains in Nelnet's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

12. Given that information relating to the Data Breach, including the systems that were impacted, the configuration and design of Defendant's website and systems remain exclusively in Defendant's control, Plaintiffs anticipate additional support for their claims will be uncovered following a reasonable opportunity for discovery.

JURISDICTION AND VENUE

13. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class and Subclass exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative Members of the Class and Subclass defined below, and a significant portion of putative Class and Subclass Members are citizens of a different state than Defendant.

14. This Court has personal jurisdiction over Defendant Nelnet because Defendant Nelnet is a resident of the State of Nebraska.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Nelnet resides in this District.

16. Plaintiffs' claims arise out of or relate to Nelnet's contacts with California. Nelnet has intentionally created extensive contacts with California through its deliberate marketing and sale of its services in the forum.

PARTIES

17. Plaintiff William Spearman ("Plaintiff Spearman") is a citizen and resident of the State of South Carolina.

18. Plaintiff Brittni Linn ("Plaintiff Linn") is a citizen and resident of the Commonwealth of Pennsylvania

19. Plaintiff Jessica Alexander ("Plaintiff Alexander") is a citizen and resident of the State of California.

20. Plaintiff Christopher Sangmeister ("Plaintiff Sangmeister") is a citizen and resident of the State of California.

21. Plaintiff Taylor Vetter ("Plaintiff Vetter") is a citizen and resident of the State of New York.

22. Plaintiff Nichole Allocca ("Plaintiff Allocca") is a citizen and resident of the State of Connecticut.

23. Plaintiff Kayli Lazard ("Plaintiff Lazard") is a citizen and resident of the State of Colorado.

24. Plaintiff Bridget Cahill ("Plaintiff Cahill") is a citizen and resident of the Commonwealth of Massachusetts.

25. Defendant Nelnet Servicing, LLC ("Nelnet") is Nebraska limited liability company with its principal place of business located at 121 South 13th Street, Suite 100, Lincoln, Nebraska, 68508.

FACTUAL BACKGROUND

I. Defendant Nelnet Servicing, LLC

26. Nelnet is a Nebraska-based company which primarily "engage[s] in student loan servicing, tuition payment processing and school information systems, and communications" and primarily makes money via "net interest income earned on a portfolio of federally insured student loans."[1] In other words, Nelnet primarily serves as a student loan servicer for individuals that have taken out federal student loans and makes money via the interest it charges individuals on their student loan balances. As of June 30, 2022, the Nelnet was servicing $589.5 billion in loans for 17.4 million borrowers.[2]

27. Nelnet also earns revenue providing technology services such as website portal and payment processing to other student loan and debt servicers, [3] such EdFinancial and the Oklahoma Student Loan Authority ("OSLA").

28. No individual voluntarily engages Nelnet as their student loan servicer or payment portal provider. Instead, Nelnet is given an individuals' federal loans to service without any choice or input given to the individual or is similarly chosen by a federal student loan servicer such as EdFinancial or OSLA to provide web portal and payment processing services without any input from the individual.

---

[1] *About Us*, NELNET, https://www.nelnetinvestors.com/Home/default.aspx (accessed Sept. 6, 2022).
[2] *Nelnet 10Q Earnings Release*, NELNET (Aug. 8, 2022) https://s21.q4cdn.com/368920761/files/doc_financials/2022/q2/8K-Exhibit-99.1-8.8.22-10Q-Earnings-Release-FINAL.pdf (accessed Sept. 6, 2022).
[3] *Id.*

II. Nelnet Obtains, Collects, and Stores Account Holders' PII

29. Nelnet requires all individuals to provide their sensitive, personal, and private protected information to register and create an account with Nelnet to use Nelnet's services.

30. Thus, all individuals whose federal student loans are assigned (without their input) to Nelnet must register with Nelnet and provide their PII to Nelnet to track and make payments on their federal student loans. Similarly, individuals whose federal student loans are serviced by a loan servicer that engages Nelnet to provide web portal or payment processing services must register and create an account with Nelnet and provide their PII to Nelnet.

31. Nelnet maintains, keeps, and exploits customers' PII for Nelnet's own benefit, including long after individuals have paid off their loans in full and cease being Nelnet customers.

32. Nelnet is in complete operation, control, and supervision of its website and systems, and Nelnet intentionally configured and designed its website and systems this way in order to make more money without regard to Plaintiffs' and Class Members' PII.

33. By obtaining, using, disclosing, and deriving a benefit from Plaintiffs' and Class Members' PII, Nelnet assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

34. Plaintiffs and Class Members reasonably expect that student loan service providers such as Nelnet will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Nelnet acknowledges that it has an obligation to protect PII from disclosure and thus makes the following representation on the Nelnet website:

> Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.[4]

36. Despite the above representations, Nelnet failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII.

37. Had Nelnet followed industry guidelines and adopted reasonably security measures as represented in the Nelnet Privacy Policy, Nelnet would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

III. FTC Guidelines

38. Nelnet is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

39. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

40. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no

[4] *Nelnet Privacy Policy Mission Statement, Our Security Procedures*, NELNET, https://www.nelnet.com/privacy-and-security#:~:text=As%20stated%20above%20we%20do,Comply%20with%20the%20law (accessed Sept 6, 2022).

longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

41. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

42. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

43. Nelnet failed to properly implement basic data security practices. Nelnet's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive Social Security information stolen, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

44. Nelnet was at all times fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and disclosing PII as well as collecting, storing, and using other confidential personal and financial information. Nelnet was also aware of the significant repercussions that would result from its failure to do so.

SUBSTANTIVE ALLEGATIONS

I. The Data Breach

45. Beginning in June 2022, Nelnet allowed an unauthorized third-party to access Plaintiffs' and Class Members' student loan account registration information, including their names, addresses, email addresses, phone numbers, and Social Security numbers. According to Nelnet, this unauthorized access continued through July 22, 2022.

46. Nelnet did not discover the unauthorized access until July 21, 2022, when Nelnet claims to have notified EdFinancial and OSLA about the vulnerability and unauthorized access.

47. Despite discovering the Data Breach July 21, 2022, Nelnet did not notify the U.S. Department of Education of the Data Breach until after August 17, 2022, and did not begin notifying impacted customers until August 26, 2022.

II. Nelnet's Data Security Failures Caused the Data Breach

48. Up to, and including, the period when the Data Breach occurred, Nelnet breached its duties, obligations, and promises to Plaintiffs and Class Members, by its failure to:

a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. properly train its employees about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;

c. address well-known warnings that its systems and servers were susceptible to a data breach;

d. implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its systems that accessed customers' personal information and otherwise would have protected customers' sensitive personal information;

e. install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented customers' sensitive personal information from being stolen. Specifically, there are recommended, available measures to prevent data from leaving protected systems and being sent to untrusted networks outside of the corporate systems; and

f. adequately safeguard customers' sensitive personal information and maintain an adequate data security environment to reduce the risk of a data breach or unauthorized disclosure.

III. Nelnet's Data Security Failures Constitute Unfair and Deceptive Practices and Violations of Consumers' Privacy Rights

49. The FTC deems the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security

problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

51. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

52. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive personal information. These orders provide further guidance to businesses regarding their data security obligations.

53. Prior to the Data Breach, and during the breach itself, Nelnet failed to follow guidelines set forth by the FTC and actively mishandled the management of its IT security.

Furthermore, by failing to have reasonable data security measures in place, Nelnet engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

IV. The Value of the Disclosed PII and Effects of Unauthorized Disclosure

54. Nelnet was well aware that the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

55. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to

commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

56. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

57. The forms of PII involved in this Data Breach are particularly concerning. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

58. Indeed, even the Social Security Administration (''SSA") warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

59. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

60. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

61. Thus, Nelnet knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Nelnet failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

62. As highly sophisticated parties that handle sensitive PII, Nelnet failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

63. Identity thieves use stolen PII for various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud and government fraud.

64. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

65. There is often a lag time between when fraud occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

66. Personal is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

67. Plaintiffs and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

68. Thus, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

V. The Data Breach Damaged Plaintiffs and Class Members.

69. As a result of Nelnet's deficient security measures, Plaintiffs and Class Members have been harmed by the compromise of their sensitive personal information, which is likely currently for sale on the dark web and through private sale to other cyber criminals.

70. Plaintiffs and Class Members also face a substantial and imminent risk of fraud and identity theft as their names have now been linked with their Social Security numbers, emails, phone numbers, and physical addresses as a result of the breach. These specific types of information are associated with a high risk of fraud.

71. Many Class Members will also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

72. Plaintiffs and Class Members also suffered a "loss of value" of their sensitive personal information when it was stolen by hackers in the Data Breach. A robust market exists for stolen personal information. Hackers sell personal information on the dark web—an underground market for illicit activity, including the purchase of hacked personal information—at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiffs and Class Members.

73. Plaintiffs' and Class Members' stolen personal information is a valuable commodity to identity thieves. William P. Barr, former United States Attorney General, made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal information is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. One commentator confirmed, explaining that,

"[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud." In fact, Plaintiffs' and Class Members' personal information is currently available for purchase on the dark web and/or through private sale to other cyber criminals.

74. Identity thieves can also combine data stolen in the Data Breach with other information about Plaintiffs and Class Members gathered from underground sources, public sources, or even Plaintiffs' and Class Members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiffs and Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining Social Security numbers in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

75. Plaintiffs and Class Members also suffered "benefit of the bargain" damages. Plaintiffs and Class Members overpaid for services that should have been—but were not—accompanied by adequate data security. Part of the interest and fees paid by Plaintiffs and Class Members to Nelnet were intended to be used to fund adequate data security. Plaintiffs and Class Members did not get what they paid for.

76. Plaintiffs and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely

than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming, especially because Nelnet has failed to disclose when the breach occurred or how long it lasted, forcing customers to continue to monitor their accounts indefinitely.

77. Class Members who experience actual identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will be harmed further by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

78. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

79. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information (including Social Security numbers) has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

80. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches to various individuals rather than in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

VI. Nelnet's Failure to Notify Plaintiffs and Class Members in a Timely or Adequate Fashion Exacerbated the Damage

81. As detailed above, Nelnet claims to have discovered the Data Breach on July 21, 2022 yet failed to even *begin* notifying Plaintiffs and Class Members until August 26, 2022 via U.S. Mail.

82. This period of over a month could have been used by Plaintiffs and Class Members to take steps to mitigate the damage caused by the Data Breach.

83. Instead, and to protect its own financial interests, Nelnet concealed the Data Breach for over a month, allowing the unauthorized third-party to potentially exploit Plaintiffs' and Class MMembers' PII without any mitigation steps being taken.

84. Plaintiffs and Class Members were deprived of the opportunity to take any steps to prevent damage by Nelnet's concealment of the Data Breach and failure to provide timely and adequate notice of the Data Breach to Plaintiffs and Class Members.

VII. Plaintiffs' Allegations

85. Plaintiff Spearman is a citizen and resident of the State of South Carolina. Plaintiff Spearman's student loans were assigned, without his input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Spearman was required to create a Nelnet account and provide PII to Nelnet in order to stay current and make payment on his student loans. Plaintiff Spearman received a letter dated

August 26, 2022 via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Spearman that his PII was compromised in the Data Breach.

86. Plaintiff Linn is a citizen and resident of the Commonwealth of Pennsylvania. Plaintiff Linn's student loans were assigned, without her input or consent, to EdFinancial for servicing in 2022. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Linn was required to create a Nelnet account and provide PII to Nelnet in order to stay current and make payment on her student loans. Plaintiff Linn received a letter dated August 26, 2022 via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Linn that her PII was compromised in the Data Breach.

87. Plaintiff Jessica Alexander ("Plaintiff Alexander") is a citizen and resident of the State of California. Plaintiff Alexander's student loans were assigned, without her input or consent, to EdFinancial. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Alexander was required to create a Nelnet account and provide PII to Nelnet in order to stay current and make payment on her student loans. Plaintiff Alexander received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Alexander that her PII was compromised in the Data Breach.

88. Plaintiff Christopher Sangmeister ("Plaintiff Sangmeister") is a citizen and resident of the State of California. Plaintiff Sangmeister's student loans were assigned, without his input or consent, to EdFinancial. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Sangmeister was required to create a Nelnet account and provide PII to Nelnet in order to stay current and make payments on his student loans. Plaintiff Sangmeister received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of

Security Incident" notifying Plaintiff Sangmeister that his PII was compromised in the Data Breach.

89. Plaintiff Taylor Vetter ("Plaintiff Vetter") is a citizen and resident of the State of New York. Plaintiff Vetter's student loans were assigned, without her input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Vetter was required to create a Nelnet account and provide PII to Nelnet. Plaintiff Vetter received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Vetter that her PII was compromised in the Data Breach.

90. Plaintiff Nichole Allocca ("Plaintiff Allocca") is a citizen and resident of the State of Connecticut. Plaintiff Allocca's student loans were assigned, without her input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Allocca was required to create a Nelnet account and provide PII to Nelnet. Plaintiff Allocca received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Allocca that her PII was compromised in the Data Breach.

91. Plaintiff Kayli Lazard ("Plaintiff Lazard") is a citizen and resident of the State of Colorado. Plaintiff Lazard's student loans were assigned, without her input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Lazard was required to create a Nelnet account and provide PII to Nelnet. Plaintiff Lazard received a letter dated August 26, 2022 via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Lazard that her PII was compromised in the Data Breach.

92. Plaintiff Bridget Cahill ("Plaintiff Cahill") is a citizen and resident of the Commonwealth of Massachusetts. Plaintiff Cahill's student loans were assigned, without her

input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Cahill was required to create a Nelnet account and provide PII to Nelnet. Plaintiff Cahill received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Cahill that her PII was compromised in the Data Breach.

CLASS ACTION ALLEGATIONS

93. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Nationwide Class").

94. Plaintiffs reserve the right to modify, expand or amend the above Nationwide Class definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

CALIFORNIA SUBCLASS

95. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following California Subclass:

> All persons in California whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "California Subclass").

96. Plaintiffs reserve the right to modify, expand or amend the above California Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

COLORADO SUBCLASS

97. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following California Subclass:

All persons in Colorado whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Colorado Subclass").

98. Plaintiffs reserve the right to modify, expand or amend the above Colorado Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

CONNECTICUT SUBCLASS

99. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Connecticut Subclass:

All persons in Connecticut whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Connecticut Subclass").

100. Plaintiffs reserve the right to modify, expand or amend the above Connecticut Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

MASSACHUSETTS SUBCLASS

101. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Massachusetts Subclass:

All persons in Massachusetts whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Massachusetts Subclass").

102. Plaintiffs reserve the right to modify, expand or amend the above Massachusetts Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

NEW YORK SUBCLASS

103. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following New York Subclass:

All persons in New York whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "New York Subclass").

104. Plaintiffs reserve the right to modify, expand or amend the above New York Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

PENNSYLVANIA SUBCLASS

105. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Pennsylvania Subclass:

All persons in Pennsylvania whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Pennsylvania Subclass").

106. Plaintiffs reserve the right to modify, expand or amend the above Pennsylvania Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

SOUTH CAROLINA SUBCLASS

107. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following South Carolina Subclass:

All persons in South Carolina whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "South Carolina Subclass").[5]

108. Plaintiffs reserve the right to modify, expand or amend the above South Carolina Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

109. Certification of Plaintiffs' claims for class-wide treatment are appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiffs can prove the elements

[5] Collectively, the California Subclass, Colorado Subclass, Connecticut Subclass, Massachusetts Subclass, New York Subclass, Pennsylvania Subclass, and South Carolina Subclass are the "State Subclasses."

of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

110. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The Members of the Nationwide Class and the State Subclasses are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While Plaintiffs are informed and believe that there are likely millions of Members of the Classes, the precise number of Class Members is unknown to Plaintiffs. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

111. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Nelnet engaged in active misfeasance and misconduct alleged herein;

b. Whether Nelnet owed a duty to Class Members to safeguard their sensitive personal information;

c. Whether Nelnet breached its duty to Class Members to safeguard their sensitive personal information;

d. Whether Nelnet knew or should have known that its data security systems and monitoring processes were deficient;

e. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of the Data Breach;

f. Whether Nelnet's failure to provide adequate security proximately caused Plaintiffs' and Class Members' injuries; and

g. Whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

112. **Typicality.** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of all Class and Subclass Members because Plaintiffs, like other Class and Subclass Members, suffered theft of their sensitive personal information in the Data Breach.

113. **Adequacy of Representation.** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are Members of the Classes and State Subclasses and their interests do not conflict with the interests of other Class and Subclass Members that they seek to represent. Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interest in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intends to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

114. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiffs' case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered

in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Nelnet, so it would be impracticable for Members of the Class to individually seek redress for Nelnet's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

115. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Nelnet has acted, or refused to act, on grounds generally applicable to the Nationwide Class and California Subclass such that final declaratory or injunctive relief is appropriate.

116. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on newly learned facts or legal developments that arise following additional investigation, discovery, or otherwise.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

117. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

118. Nelnet obtained Plaintiffs' and Class Members' sensitive personal information in connection with Plaintiffs and Class Members signing up for Nelnet's wireless services.

119. By collecting and maintaining sensitive personal information, Nelnet had a common law duty of care to use reasonable means to secure and safeguard the sensitive personal information and to prevent disclosure of the information to unauthorized individuals. Nelnet's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

120. Nelnet owed a duty of care to Plaintiffs and Class Members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

121. Nelnet's duty of care arose as a result of, among other things, the special relationship that existed between Nelnet and its customers. Nelnet was the only party in a position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur that would result in substantial harm to consumers.

122. Nelnet was subject to an "independent duty" untethered to any contract between Plaintiffs and Class Members and Nelnet.

123. 91. Nelnet breached its duties, and thus was negligent, by failing to use reasonable measures to protect customers' sensitive personal information. Nelnet's negligent acts and omissions include, but are not limited to, the following:

a. failure to employ systems and educate employees to protect against malware;

b. failure to comply with industry standards for software and server security;

c. failure to track and monitor access to its network and personal information;

d. failure to limit access to those with a valid purpose;

e. failure to adequately staff and fund its data security operation;

f. failure to remove, delete, or destroy highly sensitive personal information of consumers that is no longer being used for any valid business purpose;

g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

h. failure to recognize that hackers were stealing personal information from its network while the Data Breach was taking place.

124. It was foreseeable to Nelnet that a failure to use reasonable measures to protect its customers' sensitive personal information could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Nelnet given the known frequency of data breaches and various warnings from industry experts.

125. As a direct and proximate result of Nelnet's negligence, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

126. Plaintiffs and Class Members are also entitled to injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

127. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

129. Nelnet violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Nelnet's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

130. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

131. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

132. As a direct and proximate result of Nelnet's negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

133. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

134. Plaintiffs and Class Members are also entitled to injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

135. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

136. When Plaintiffs and Class Members provided their sensitive personal information to Nelnet in exchange for Nelnet's services, they entered into implied contracts with Nelnet under which Nelnet agreed to take reasonable steps to protect their sensitive personal information.

137. Nelnet solicited and invited Plaintiffs and Class Members to provide their sensitive personal information as part of Nelnet's regular business practices. Indeed, to sign up for a Nelnet account—which is required to make payments online to loan serviced by companies that hire Nelnet for web portal and payment processing services—Nelnet requires customers to provide sensitive personal information including Social Security numbers, to obtain Nelnet's services. Plaintiffs and Class Members accepted Nelnet's offers and provided their sensitive personal information Nelnet.

138. Plaintiffs and Class Members reasonably believed and expected that Nelnet's data security practices complied with relevant laws, regulations, and industry standards when they entered into the implied contracts with Nelnet.

139. Plaintiffs and Class Members paid money to Nelnet and Plaintiffs and Class Members therefore reasonably believed and expected that Nelnet would use part of those funds to obtain adequate data security. Nelnet failed to do so.

140. Plaintiffs and Class Members would not have provided their sensitive personal information to Nelnet in the absence of Nelnet's implied promise to keep their sensitive personal information reasonably secure.

141. Plaintiffs and Class Members fully performed their obligations under the implied contracts by paying money to Nelnet.

142. Nelnet breached its implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures.

143. As a direct and proximate result of Nelnet's breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

144. Plaintiffs and Class Members are also entitled to injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

145. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

146. Plaintiffs and Class Members conferred a monetary benefit upon Nelnet in the form of monies paid in the course of utilizing Nelnet's online services.

147. Nelnet appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Nelnet also benefited from the receipt of Plaintiffs' and Class

Members' sensitive personal information as this was utilized by Nelnet to send bills and process payments for services, among other things.

148. The monies Plaintiffs and Class Members paid to Nelnet were supposed to be used by Nelnet, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

149. Nelnet's conduct caused Plaintiffs and Class Members to suffer actual damages in an amount equal to the difference in value between what they paid for (Nelnet's services made with adequate data privacy and security practices and procedures), and what they actually received (Nelnet's services without adequate data privacy and security practices and procedures).

150. In equity and good conscience, Nelnet should not be permitted to retain the money belonging to Plaintiffs and Class Members because Nelnet failed to implement, or adequately implement, the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

151. Nelnet should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF CONFIDENCE
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

152. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

153. Plaintiffs and Class Members maintained a confidential relationship with Nelnet whereby Nelnet undertook a duty not to disclose to unauthorized parties the PII provided by

Plaintiffs and Class Members to Nelnet to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

154. Nelnet knew Plaintiffs' and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

155. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because Nelnet failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

156. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

157. But for Nelnet's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Nelnet's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

158. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Nelnet's unauthorized disclosure of Plaintiffs' and Class Members' PII. Nelnet knew its computer systems and technologies for accepting, securing, and storing

COUNT VI
INVASION OF PRIVACY – INSTUSION UPON SECLUSION
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

159. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

160. Plaintiffs shared PII with Nelnet that Plaintiffs wanted to remain private and non-public.

161. Plaintiffs reasonably expected that the PII they shared with Nelnet would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

162. Nelnet intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party who then sold their PII to other third-parties on the dark web.

163. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Nelnet unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

164. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included Social Security numbers and other PII.

165. Nelnet's intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

166. As a direct and proximate result of Nelnet's invasions of privacy, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Nelnet; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Nelnet's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT VII
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA"),
Cal. Civ. Code §§ 1798.150, *et seq.*
(On behalf of the Plaintiff Sangmeister, Plaintiff Alexander and the California Subclass)

167. Plaintiff Sangmeister and Plaintiff Alexander, individually and on behalf of the California Subclass, repeat and reallege all preceding allegations as if fully set forth herein.

168. Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members are residents of California.

169. Nelnet is a corporation organized or operated for the profit or financial benefit of its owners. Nelnet collects consumers' personal information ("PII" for purposes of this Count) as defined in Cal. Civ. Code § 1798.140.

170. Nelnet violated § 1798.150 of the CCPA by failing to prevent Plaintiff Sangmeister's and Plaintiff Alexander's and the Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Nelnet's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

171. Nelnet has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Sangmeister's and Plaintiff Alexander's and Subclass Members' PII. As detailed herein, Nelnet failed to do so.

172. As a direct and proximate result of Nelnet's acts, the PII of Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members, including social security numbers, phone numbers, names, addresses, and email addresses, was subjected to unauthorized access and exfiltration, theft, or disclosure.

173. Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members seek injunctive or other equitable relief to ensure Nelnet hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Nelnet continues to hold customers' PII, including Plaintiff Sangmeister's and Plaintiff Alexander's and California Subclass Members' PII. Plaintiff Sangmeister and Plaintiff Alexander and Subclass Members have an interest in ensuring that

their PII is reasonably protected, and Nelnet has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

174. As described herein, an actual controversy has arisen and now exists as to whether Nelnet implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

175. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Nelnet and third parties with similar inadequate security measures.

176. Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass seek statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

177. Plaintiff Sangmeister and Plaintiff Alexander have also provided written notice to Defendant identifying the specific provisions of the CCPA that it has violated. If Defendant fails to respond to Plaintiff Sangmeister's and Plaintiff Alexander's notice letter or fails to agree to adequately cure the violations described herein (and to certify that no further violations will occur), Plaintiff Sangmeister and Plaintiff Alexander will also seek statutory damages on behalf of themselves and the California Subclass.

COUNT VIII
CALIFORNIA CUSTOMER RECORDS ACT.
Cal. Civ. Code §§ 1798.80, *et seq.*
(On behalf of the Plaintiff Sangmeister, Plaintiff Alexander and the California Subclass)

178. Plaintiff Sangmeister and Plaintiff Alexander, individually and on behalf of the California Subclass, repeat and reallege all preceding allegations as if fully set forth herein.

179. Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members are residents of California.

180. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure."

181. Nelnet is a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members.

182. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of PII that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

183. Nelnet is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

184. Plaintiff Sangmeister's and Plaintiff Alexander's and California Subclass Members' PII (e.g., Social Security numbers) includes PII as covered by Cal. Civ. Code § 1798.82.

185. Because Nelnet reasonably believed that Plaintiff Sangmeister's and Plaintiff Alexander's and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Nelnet had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

186. Nelnet failed to fully disclose material information about the Data Breach, including the types of PII impacted, in a timely fashion.

187. By failing to disclose the Data Breach in a timely and accurate manner, Nelnet violated Cal. Civ. Code § 1798.82.

188. As a direct and proximate result of Nelnet's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members suffered damages, as described above.

189. Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT IX
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On behalf of the Plaintiff Sangmeister, Plaintiff Alexander and the California Subclass)

190. Plaintiff Sangmeister and Plaintiff Alexander, individually and on behalf of the California Subclass, repeat and reallege all preceding allegations as if fully set forth herein.

191. Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members are residents of California.

192. Plaintiff Sangmeister and Plaintiff Alexander re-alleges and incorporate by reference all preceding allegations as if fully set forth herein.

193. Nelnet is a "person" as defined by Cal. Bus. & Prof. Code §17201.

194. Nelnet violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

195. Nelnet's "unfair" acts and practices include:

a. Nelnet failed to implement and maintain reasonable security measures to protect Plaintiff Sangmeister's and Plaintiff Alexander's and Subcllass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Nelnet failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Sangmeister and Plaintiff Alexander and Subclass Members, whose PII has been compromised.

c. Nelnet's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. Nelnet's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Nelnet's grossly inadequate security, consumers could not have reasonably avoided the harms that Nelnet caused.

196. Nelnet engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

197. Nelnet has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

198. Nelnet's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Sangmeister's and Plaintiff Alexander's and

Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Sangmeister's and Plaintiff Alexander's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Sangmeister's and Plaintiff Alexander's Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Sangmeister's and Plaintiff Alexander's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Sangmeister's and Plaintiff's Alexander and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security

and privacy of Plaintiff Sangmeister's and Plaintiff Alexander's Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and 1798.81.5, which was a direct and proximate cause of the Data Breach.

199. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

200. As a direct and proximate result of Nelnet's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

201. Nelnet acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members' rights. Nelnet's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

202. Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Nelnet's unfair, unlawful, and fraudulent business practices or use of their PII;

declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT X
VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750, *et seq.*
(On behalf of Plaintiff Sangmeister, Plaintiff Alexander and the California Subclass)

203. Plaintiff Sangmeister and Plaintiff Alexander, individually and on behalf of the California Subclass, repeat and reallege all preceding allegations as if fully set forth herein.

204. Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members are residents of California.

205. 343. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*, ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

206. 344. Nelnet is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

345. Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

207. Nelnet's acts and practices were intended to and did result in the sales of products and services to Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass Members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

208. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

209. Had Nelnet disclosed to Plaintiff Sangmeister and Plaintiff Alexander and California Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

210. As a direct and proximate result of Nelnet's violations of California Civil Code § 1770, Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft;

time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

211. Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass intends to seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

212. Plaintiff Sangmeister and Plaintiff Alexander and the California Subclass, further intends to seek compensatory and punitive damages. Pursuant to Cal. Civ. Code § 1782(a), Plaintiffs intend to serve Nelnet with notice of their alleged violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date of such notification, Nelnet fails to provide appropriate relief for its violations of the CLRA, Plaintiff Sangmeister and Plaintiff Alexander will amend this Complaint to seek monetary damages.

COUNT XI
COLORADO SECURITY BREACH NOTIFICATION ACT
Colo. Rev. Stat. §§ 6-1-716, *et seq.*
(On behalf of Plaintiff Lazard and the Colorado Subclass)

213. Plaintiff Lazard individually and on behalf of the Colorado Subclass, repeats and realleges all allegations as if fully set forth herein.

214. Nelnet is a business that owns or licenses computerized data that includes PII as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

215. The PII of Plaintiff Lazard and the Colorado Subclass (*e.g.*, Social Security numbers) includes PII as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

216. Nelnet is required to accurately notify Plaintiff Lazard and the Colorado Subclass if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

217. Because Nelnet was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

218. By failing to disclose the Data Breach in a timely and accurate manner, Nelnet violated Colo. Rev. Stat. § 6-1-716(2).

219. As a direct and proximate result of Nelnet's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff Lazard and Colorado Subclass Members suffered damages, as described above.

220. Plaintiff Lazard and the Colorado Subclass Members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

COUNT XII
COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §§ 6-1-101, *et seq.*
(On behalf of Plaintiff Lazard and the Colorado Subclass)

221. Plaintiff Lazard individually and on behalf of the Colorado Subclass, repeats and realleges all allegations as if fully set forth herein.

222. Nelnet is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

223. Nelnet engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

224. Plaintiff Lazard and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by Nelnet or successors in interest to actual consumers.

225. Nelnet engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Nelnet knew or should have known that there were or another;

c. Advertising services with intent not to sell them as advertised;

d. Employing "bait and switch" advertising, which is advertising accompanied by an effort to sell goods, services, or property other than those advertised or on terms other than those advertised; and

e. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

226. Nelnet's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Lazard's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Lazard's and Subclass Members' PII,

including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Lazard's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Lazard's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Lazard and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Lazard's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

227. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

228. Nelnet intended to mislead Plaintiff Lazard and Colorado Subclass Members and induce them to rely on its misrepresentations and omissions.

229. Had Nelnet disclosed to Plaintiff Lazard and the Colorado Subclass that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to

continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Lazard and the Colorado Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Lazard and the Colorado Subclass Members acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

230. Nelnet acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff Lazard's and Colorado Subclass Members' rights. Nelnet's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

231. As a direct and proximate result of Nelnet's deceptive trade practices, Plaintiff Lazard and the Colorado Subclass suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII, monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

232. Nelnet's deceptive trade practices significantly impact the public, because many Members of the public are actual or potential consumers of Nelnet's services and the Data Breach affected millions of Americans, which include Members of the Colorado Subclass.

233. Plaintiff Lazard and the Colorado Subclass seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XIII
CONNECTICUT UNFAIR TRADE PRACTICES ACT
Conn. Gen. Stat. Ann. §§ 42-110a *et seq.*
(On behalf of Plaintiff Allocca and the Connecticut Subclass)

234. Plaintiff Allocca individually, and on behalf of the Connecticut Subclass, repeats and realleges all allegations as if fully set forth herein.

235. Nelnet is a "person" as defined by Conn. Gen. Stat. Ann. § 42-110(a)(3).

236. Plaintiff Allocca and Connecticut Subclass Members are actual or potential consumers of Recalled Devices.

237. At all times mentioned herein, Nelnet engages in "trade" or "commerce" in Connecticut as defined by Conn. Gen. Stat. Ann. § 42-110(a)(4), in that they engaged in the "advertising," "sale," and "distribution" of any "goods," "services," "property," "articles," "commodities," or "things of value" in Connecticut.

238. The Connecticut Unfair Trade Practices Act (CUTPA) provides that "[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." C.G.S.A. § 42-110b(a).

239. For the reasons discussed herein, Nelnet violated CUTPA by engaging in the herein described deceptive or unfair acts or practices proscribed by § 42-110a *et seq.* Nelnet's acts and practices, including its material omissions, described herein, were likely to, and did in fact, deceive and mislead Members of the public, including consumers acting reasonably under the circumstances, to their detriment.

240. Nelnet engaged in deceptive trade practices in the course of its business, in violation of CUTPA, including:

a. Making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Nelnet knew or should have known that there were or another;

c. Advertising services with intent not to sell them as advertised;

d. Employing "bait and switch" advertising, which is advertising accompanied by an effort to sell goods, services, or property other than those advertised or on terms other than those advertised; and

e. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

241. Nelnet's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Allocca's and Connecticut Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Allocca's and Connecticut Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Allocca's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Allocca's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Allocca's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Allocca's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

242. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

243. Nelnet intended to mislead Plaintiff Allocca and Connecticut Subclass Members and induce them to rely on its misrepresentations and omissions.

244. Had Nelnet disclosed to Plaintiff Allocca and the Connecticut Subclass that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Allocca and the Connecticut Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Allocca and the Connecticut Subclass Members acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

245. Nelnet acted intentionally, knowingly, and maliciously to violate CUTPA, and recklessly disregarded Plaintiff Allocca and Connecticut Subclass Members' rights. Nelnet's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

246. As a direct and proximate result of Nelnet's deceptive trade practices, Plaintiff Allocca and the Connecticut Subclass suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII, monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

247. Nelnet's deceptive trade practices significantly impact the public, because many Members of the public are actual or potential consumers of Nelnet's services and the Data Breach affected millions of Americans, which include Members of the Colorado Subclass.

248. Plaintiff Allocca and the Connecticut Subclass seek relief for the injuries they have suffered as a result of Nelnet's unfair and deceptive acts and practices, as provided by C.G.S.A. § 42-110g and applicable law.

COUNT XIV
MASSACHUSETTS CONSUMER PROTECTION ACT,
Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.*
(On behalf of Plaintiff Cahill and the Massachusetts Subclass)

249. Plaintiff Cahill, individually and on behalf of the Massachusetts Subclass, repeats and realleges all allegations as if fully set forth herein.

250. Nelnet and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

251. Nelnet operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

252. Nelnet advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

253. Nelnet engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Cahill's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cahill's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Cahill's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cahill's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Cahill's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cahill's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

254. Nelnet's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Nelnet solely held the true facts about its inadequate security for PII, which Plaintiff Cahill and the Massachusetts Subclass could not independently discover.

255. Consumers could not have reasonably avoided injury because Nelnet's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Nelnet created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

256. Nelnet's inadequate data security had no countervailing benefit to consumers or to competition.

257. Nelnet intended to mislead Plaintiff Cahill and the Massachusetts Subclass and induce them to rely on its misrepresentations and omissions. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

258. Nelnet acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff Cahill's and Massachusetts Subclass Members' rights.

259. As a direct and proximate result of Nelnet's unfair and deceptive, Plaintiff Cahill and the Massachusetts Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

260. Plaintiff Cahill and the Massachusetts Subclass seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

COUNT XV
NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.*
(On behalf of Plaintiff Vetter and the New York Subclass)

261. Plaintiff Vetter individually, and on behalf of the New York Subclass, repeats and realleges all allegations as if fully set forth herein.

262. Nelnet engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Vetter's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Vetter's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Vetter's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Vetter's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Vetter's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Vetter's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

263. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

264. Nelnet acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff Vetter's and New York Subclass Members' rights.

265. As a direct and proximate result of Nelnet's deceptive and unlawful acts and practices, Plaintiff Vetter and the New York Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

266. Nelnet's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

267. The above deceptive and unlawful practices and acts by Nelnet caused substantial injury to Plaintiff Vetter and the New York Subclass that they could not reasonably avoid.

268. Plaintiff Vetter and the New York Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs

COUNT XVI
PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,
73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*
(On behalf of Plaintiff Linn and the Pennsylvania Subclass)

269. Plaintiff Linn individually, and on behalf of the Pennsylvania Subclass, repeats and realleges all allegations as if fully set forth herein.

270. Nelnet is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

271. Plaintiff Linn and the Pennsylvania Subclass purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

272. Nelnet engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

273. Nelnet's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Linn's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Linn's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Linn's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Linn's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Linn's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Linn's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

274. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

275. Nelnet intended to mislead Plaintiff Linn and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

276. Had Nelnet disclosed to Plaintiff Linn and the Pennsylvania Subclass that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Linn and the Pennsylvania Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Linn and the Pennsylvania Subclass acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

277. Nelnet acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff Linn's and Pennsylvania Subclass Members' rights.

278. As a direct and proximate result of Nelnet's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff Linn's and the Pennsylvania Subclass' reliance on them, Plaintiff Linn and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased,

imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

279. Plaintiff Linn and the Pennsylvania Subclass seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

COUNT XVII
SOUTH CAROLINA DATA BREACH SECURITY ACT,
S.C. Code Ann. §§ 39-1-90, *et seq.*
(On behalf of Plaintiff Spearman and the South Carolina Subclass)

280. Plaintiff Spearman individually, and on behalf of the South Carolina Subclass, repeats and realleges all allegations if fully set forth herein.

281. Nelnet is a business that owns or licenses computerized data or other data that includes personal identifying information (for the purpose of this count, "PII"), as defined by S.C. Code Ann. § 39-1-90(A).

282. Plaintiff Spearman's and South Carolina Subclass Members' PII (*e.g.,* Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

283. Nelnet is required to accurately notify Plaintiff Spearman and South Carolina Subclass Members following discovery or notification of a breach of its data security system if PII that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

284. Because Nelnet discovered a breach of its data security system in which PII that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Nelnet had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

285. By failing to disclose the Data Breach in a timely and accurate manner, Nelnet violated S.C. Code Ann. § 39-1-90(A).

286. As a direct and proximate result of Nelnet's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff Spearman and South Carolina Subclass Members suffered damages, as described above.

287. Plaintiff Spearman and South Carolina Subclass Members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT XVIII
SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT,
S.C. Code Ann. §§ 39-5-10, *et seq.*
(On behalf of Plaintiff Spearman and the South Carolina Subclass)

288. Plaintiff Spearman individually, and on behalf of the South Carolina Subclass, repeats and realleges all allegations if fully set forth herein.

289. Nelnet is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

290. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

291. Nelnet advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

292. Nelnet engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Spearman's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Spearman's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Spearman's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Spearman's and South Carolina Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Spearman's and South Carolina Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security

and privacy of Plaintiff Spearman's and South Carolina Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

293. Nelnet's acts and practices had, and continue to have, the tendency or capacity to deceive.

294. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

295. Nelnet intended to mislead Plaintiff Spearman and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

296. Had Nelnet disclosed to Plaintiff Spearman and the South Carolina Subclass that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Spearman and the South Carolina Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Spearman and the South Carolina Subclass acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

297. Nelnet had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiff Spearman and the South Carolina Subclass—and Nelnet, because consumers are unable to fully protect their interests with regard to the PII in

Nelnet's possession and placed trust and confidence in Nelnet. Nelnet's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the South Carolina Subclass that contradicted these representations.

298. Nelnet's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Nelnet's acts and practices offend established public policies that seek to protect consumers' PII and ensure that entities entrusted with PII use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45; and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, *et seq*.

299. Nelnet's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive given the sensitivity and extensivity of PII in its possession; its special role as a linchpin of the financial system; and its admitted duty of trustworthiness and care as an entrusted protector of data.

300. Nelnet's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Nelnet engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including many South Carolinians impacted by the Data Breach.

301. Nelnet's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Nelnet's policies and procedures, such as its security practices, create the potential for recurrence of the complained of business acts and practices.

302. Nelnet's violations present a continuing risk to Plaintiffs and South Carolina Subclass Members as well as to the general public.

303. Nelnet intended to mislead Plaintiff Spearman and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

304. Nelnet acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff Spearman and South Carolina Subclass Members' rights. Nelnet's numerous past data breaches put it on notice that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct and would deter Nelnet and others from committing similar conduct in the future.

305. As a direct and proximate result of Nelnet's unfair and deceptive acts or practices, Plaintiff Spearman and South Carolina Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

306. Plaintiff Spearman and South Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XIX
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of the Nationwide Class, or alternatively, the State Subclasses)

307. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

308. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

309. An actual controversy has arisen in the wake of the Data Breach regarding Nelnet's present and prospective common law and statutory duties to reasonably safeguard its customers' sensitive personal information and whether Nelnet is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches. Plaintiffs alleges that Nelnet's data security practices remain inadequate.

310. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

311. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Nelnet continues to owe a legal duty to secure consumers' sensitive personal information, to timely notify consumers of any data breach, and to establish

and implement data security measures that are adequate to secure customers' sensitive personal information.

312. The Court also should issue corresponding prospective injunctive relief requiring Nelnet to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

313. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach at Nelnet occurs, Plaintiffs and Class Members will not have an adequate remedy at law, because not all of the resulting injuries are readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

314. The hardship to Plaintiffs and Class Members if an injunction does not issue greatly exceeds the hardship to Nelnet if an injunction is issued. If another data breach occurs at Nelnet, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Nelnet of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Nelnet has a pre-existing legal obligation to employ such measures.

315. Issuance of the requested injunction will serve the public interest by preventing another data breach at Nelnet, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

REQUEST FOR RELIEF

316. Plaintiffs, on behalf of all others similarly situated, request that the Court enter judgment against Nelnet including the following:

A. Determining that this matter may proceed as a class action and certifying the Classes asserted herein;

B. Appointing Plaintiffs as representative of the applicable Classes and appointing Plaintiffs' counsel as Class counsel;

C. An award to Plaintiffs and the Classes of compensatory, consequential, statutory, restitutionary, and treble damages as set forth above;

D. Ordering injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members; (iv) timely notify consumers of any future data breaches; and (v) delete or destroy any legacy consumer data that it is not necessary to keep for business purposes;

E. Entering a declaratory judgment stating that Nelnet owes a legal duty to secure consumers' sensitive personal information, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

317. Plaintiffs demands a trial by jury for all issues so triable.

DATED this 7th day of September, 2022.

WILLIAM SPEARMAN, BRITTNI LINN, JESSICA ALEXANDER, CHRISTOPHER SANGMEISTER, TAYLOR VETTER, NICHOLE ALLOCCA, KAYLI LAZARD, and BRIDGET CAHILL, individually and on behalf of all others similarly situated, Plaintiffs

/s/ Joel M. Carney

Joel M. Carney, #21922
Jeana L. Goosmann, #22545
Joseph V. Messineo, #21981
GOOSMANN LAW FIRM, PLC
17838 Burke Street, Ste. 250
Omaha, NE 68118
Telephone: (402) 280-7648
carneyj@goosmannlaw.com
goosmannj@goosmannlaw.com
messineoj@goosmannlaw.com

and

Steven L. Bloch (*pro hac vice* forthcoming)
Ian W. Sloss (*pro hac vice* forthcoming)
Zachary Rynar (*pro hac vice* forthcoming)
SILVER GOLUB & TEITELL LLP
One Landmark Square
Fifteenth Floor
Stamford, Connecticut 06901
Telephone: (203) 325-4491
Fax: (203) 325-3769
sbloch@sgtlaw.com
isloss@sgtlaw.com
zrynar@sgtlaw.com

Christian Levis
Johnathan Seredynski
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Fax: (914) 997-0035

clevis@lowey.com
jseredynski@lowey.com

Anthony M. Christina
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com